

Appl. No.: 09/944,694
Amdt. dated 08/16/2005
Reply to Official Action of March 16, 2005

REMARKS/ARGUMENTS

Applicant appreciates the thorough examination of the present application, as evidenced by the first Official Action. In this regard, the first Official Action rejects all of the pending claims of the present application, namely Claims 1-18, under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,772 to Binding et al. In response to the first Official Action, Applicant has amended independent Claims 1, 2 and 3 to more clearly define the claimed invention. As explained below, Applicant respectfully submits that amended independent Claims 1, 2 and 3, and by dependency Claims 4-18, are patentably distinct from the Binding patent. In view of the amendments to the claims and the remarks presented herein, Applicant respectfully requests reconsideration and allowance of all of the pending claims of the present application.

Briefly, the Binding patent discloses a piggy-backed key exchange protocol for providing low-overhead browser connections from a client to a server using a trusted third party. According to one disclosed scenario implementing the disclosed system, a client and server do not have a common message encoding scheme with one another. However, each of the client and server does share an encoding scheme with a trusted third party (TTP), M1 representing the encoding scheme between the client and TTP, and M2 representing the encoding scheme between the TTP and server. In accordance with this disclosed scenario, the client sends the server a common HTTP message (e.g., HTTP GET) that includes security-sensitive parameters encrypted using scheme M1. The server, determining that it cannot process the encrypted parameters, encrypts the encrypted parameters using scheme M2, and forwards the further-encrypted parameters to the TTP. Being configured to process messages encrypted with either scheme M1 or scheme M2, the TTP decrypts the further-encrypted parameters using scheme M2, and then decrypts the encrypted parameters using scheme M1, the decryption steps resulting in cleartext parameters.

Further in accordance with the Binding patent, after obtaining the cleartext parameters, the TTP re-encrypts the cleartext parameters using scheme M2, and forwards the re-encrypted parameters to the server. The server decrypts the re-encrypted parameters using scheme M2 to similarly obtain the cleartext parameters, from which the server creates the content requested by

Appl. No.: 09/944,694
Amdt. dated 08/16/2005
Reply to Official Action of March 16, 2005

the client. The server then encrypts the requested content using a new encryption scheme M3, thereafter returning, to the client, the encrypted content as well as meta-information describing scheme M3. The client uses the meta-information to determine how to decrypt the requested content, and accordingly decrypts the requested content using scheme M3.

The present application presents a system and method for providing network security. As recited by amended independent Claim 1, a method for providing network security includes receiving a plurality of network protocol packets (e.g., IP packets). A network protocol packet includes a network protocol header (e.g., IP header) and a plurality of network protocol data, which includes a first cryptographic protocol header (e.g., TCP header) and a first plurality of encrypted data (e.g., SSL data). As amended, at least a portion of some of the network protocol packets are configured in accordance with a transport layer protocol (e.g., TCP/UDP) or a network layer protocol (e.g., IP). As also recited, a first plurality of cryptographic protocol rules (e.g., WTLS rules) associated with the network protocol data is determined, with a cryptographic session being established if required by the first cryptographic rules. The first plurality of cryptographic protocol rules are applied to the first encrypted data to obtain a first plurality of cleartext data (e.g., WML data). The first plurality of cleartext data is translated into a second plurality of cleartext data (e.g., HTML data) in accordance with at least one translation rule. The second plurality of cleartext data is then encrypted in accordance with at least one rule associated with a second cryptographic protocol (e.g., HTTP over SSL), resulting in a second plurality of encrypted data.

Generally, in contrast to the claimed invention's handling of security at the transport layer (e.g., TCP/UDP) or the network protocol layer (e.g., IP), the Binding patent provides a system and method for providing security at the application layer (e.g., HTTP), while in the claimed invention the security is handled on transport protocol layer (TCP/UDP) or on network protocol layer (IP). More particularly, in contrast to the method of independent Claim 1, the Binding patent does not teach or suggest performing cryptographic operations (i.e., determining cryptographic rules, establishing a cryptographic session, applying the cryptographic rules, etc.) based on network protocol packets at least a portion of some of which are configured in accordance with a transport layer protocol or a network layer protocol. In this regard, as

Appl. No.: 09/944,694
Amdt. dated 08/16/2005
Reply to Official Action of March 16, 2005

disclosed by the Binding patent, transport-based security protocols such as WTLS (see Claim 6) and SSL (see Claim 9) are ineffective in environments having transcoders and gateways that must inspect and thereafter modify some non-security-sensitive sections of a data stream. As also disclosed, to enable an intermediary to perform content modifications, end-to-end security must be provided at the application layer. Binding Patent, col. 3, lines 3-24. Accordingly, the Binding patent discloses a system and method that establishes and maintains end-to-end security sessions at the application layer, while maintaining the integrity of an application-layer protocol and avoiding adding amounts of communication and message exchanges. *Id.* at col. 4, lines 9-14. More particularly, as indicated above, the Binding patent discloses that a client piggy-backs security-sensitive parameters onto application-layer message headers, such as common HTTP message (e.g., HTTP GET) headers. In contrast, the claimed invention recites that at least a portion of some of the received network protocol packets are configured in accordance with a transport layer protocol (e.g., TCP/UDP) or a network layer protocol (e.g., IP).

In addition to the configuration of at least a portion of some of the network protocol packets, the Binding patent does not teach or suggest translating a first plurality of cleartext data (e.g., associated with WML) into a second plurality of cleartext data (e.g., associated with HTML) in accordance with at least one translation rule, as also recited by amended independent Claim 1. The Official Action cites column 15, lines 52 – 59 of the Binding patent as disclosing this feature of the claimed invention. In this regard, the cited passage of the Binding patent discloses a TTP encrypting security-sensitive parameters using scheme M2, where a server from which a client requested content later decrypts the parameters and uses them to create the requested content that can then be encrypted and provided to the client. The Binding patent therefore discloses creating requested content based upon security-sensitive parameters. The Binding patent does not disclose, however, translating a first plurality of cleartext data into a second plurality of cleartext data. More particularly, even if it could reasonably be suggested that the disclosed security-sensitive parameters and requested content correspond to a first and second plurality of cleartext data, respectively, the Binding patent can not reasonably be interpreted to disclose not teach or suggest translating the security-sensitive parameters into the requested data, as recited by the claimed invention.

Appl. No.: 09/944,694
Amdt. dated 08/16/2005
Reply to Official Action of March 16, 2005

Applicant therefore respectfully submits that the method of amended independent Claim 1, and by dependency Claims 4-11, is patentably distinct from the system and method of the Binding patent. Applicant also respectfully submits that amended independent Claims 2 and 3, and by dependency Claims 12-18, recite subject matter similar to that of amended independent Claim 1. For example, amended independent Claim 2 recites that at least a portion of at least some of the received network protocol packets are configured in accordance with a transport layer protocol or a network layer protocol. Also, for example, amended independent Claim 3 recites obtaining first cleartext data based upon first encrypted data, translating the first cleartext data into second cleartext data, and encrypting the second cleartext data to obtain second encrypted data. As such, Applicant respectfully submits that amended independent Claims 2 and 3, and by dependency Claims 12-18, are patentably distinct from the Binding patent for at least those reasons explained above with respect to amended independent Claim 1.

In addition to the aforementioned reasons, Applicant respectfully submits that various ones of dependent Claims 4-11 recite features that are further patentably distinct from the system and method of the Binding patent. For example, dependent Claims 6 and 9 further recite that the first and second cryptographic protocols comprise WTLS and SSL over HTTP, respectively. As will be appreciated, and as explained in the Binding patent, WTLS and SSL are both transport-layer security protocols. As also explained by the Binding patent, however, such protocols have drawbacks in certain environments, which the Binding patent seeks to overcome by establishing and maintaining end-to-end security sessions at the application layer. Thus, although the Binding patent does disclose the existence of the WTLS and SSL protocols, the Binding patent teaches away from their use by implementing its disclosed application-layer security system and method.

Applicant therefore respectfully submits that the rejection of Claims 1-18 under 35 U.S.C. § 102(e) as being anticipated by the Binding patent is overcome.

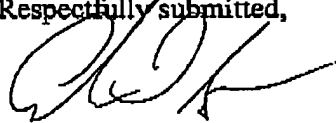
Appl. No.: 09/944,694
Amdt. dated 08/16/2005
Reply to Official Action of March 16, 2005

CONCLUSION

In view of the amendments to the claims and the remarks presented above, Applicant respectfully submits that the present application is in condition for allowance. As such, the issuance of a Notice of Allowance is therefore respectfully requested. In order to expedite the examination of the present application, the Examiner is encouraged to contact Applicant's undersigned attorney in order to resolve any remaining issues.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,




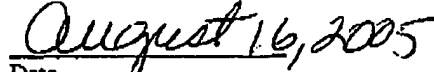
Andrew T. Spence
Registration No. 45,699

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this paper is being facsimile transmitted to the US Patent and Trademark Office at Fax No. (571) 273-8300 on the date shown below.


Sarah B. Simmons


Date